

# EXHIBIT A

1 PACIFIC TRIAL ATTORNEYS  
A Professional Corporation  
2 Scott J. Ferrell, Bar No. 202091  
sferrell@pacifictrialattorneys.com  
3 4100 Newport Place Drive, Ste. 800  
Newport Beach, CA 92660  
4 Tel: (949) 706-6464  
Fax: (949) 706-6469

5 Attorneys for Plaintiff

Electronically FILED by  
Superior Court of California,  
County of Los Angeles  
1/18/2024 8:06 AM  
David W. Slayton,  
Executive Officer/Clerk of Court,  
By E. Galicia, Deputy Clerk

8 **SUPERIOR COURT FOR THE STATE OF CALIFORNIA**  
9 **COUNTY OF LOS ANGELES**

11 MILTITA CASILLAS,

12 Plaintiff,

13 v.

14 HANESBRANDS INC., a Maryland corporation  
d/b/a WWW.MAIDENFORM.COM,

15 Defendant.

Case No. **24STCV01291**

**COMPLAINT FOR VIOLATION OF  
CALIFORNIA INVASION OF PRIVACY  
ACT ("CIPA")**

## I. INTRODUCTION

Defendant has secretly deployed spyware at www.maidenform.com that accesses visitors' devices, installs tracking spyware, and then monitors and reports visitors' online habits *after* they leave the Website.

Plaintiff recently visited Defendant's website. Without Plaintiff's knowledge or consent, Defendant secretly accessed Plaintiff's device and installed "pen register" and "trap and trace" tracking software in violation of California law. The harm caused by this intrusion is grave, as summarized by the world's leading cybersecurity firm:

*Data is worth money, which is a major reason that your online privacy is under threat.*

*For instance, knowing your browsing habits or search history can deliver big profits to advertisers. If you've been searching for new apartments, your search history could tip an advertiser off to the fact that you're going to be moving home soon — time to start serving you ads for moving services, furniture, DIY stores, and home insurance.*

*The risks are more far-reaching than most people realize because of what might happen to your data next. The development of Big Data means that your browsing history could be analyzed to come up with conclusions that you don't want to be drawn. For example, a woman buying items such as folic acid supplements might not appreciate a marketing agency identifying her as 'pregnant' and targeting her with pregnancy products. If she's living with mom and dad or hasn't told her partner, she might not be happy to see 'Congratulations on Your Baby!' marketing materials arrive in the mail.*

*Whenever you visit a website, data is being stored about you — possibly without your consent and even without your knowledge. You likely want to know where that data goes and how it's used, or you could decide you want to avoid it being collected altogether.<sup>1</sup>*

## II. JURISDICTION AND VENUE

1. Defendant is subject to jurisdiction in this state under Penal Code section 502(j), which provides that a person who accesses a computer from another jurisdiction is deemed to have personally

<sup>1</sup> Excerpted from "What Is Data Privacy?", found online at <https://usa.kaspersky.com/resource-center/threats/internet-and-individual-privacy-protection> (last accessed January 2024).

1 accessed the computer in California. Plaintiff was in California when Defendant accessed Plaintiff's  
2 device and installed tracking code.

3 2. Defendant is also subject to jurisdiction under California's "long-arm" statute found at  
4 California Code of Civil Procedure section 410.10 because the exercise of jurisdiction over Defendant  
5 is not "inconsistent with the Constitution of this state or the United States." Indeed, Plaintiff believes  
6 that Defendant generates a minimum of eight percent of revenues from its website based upon  
7 interactions with Californians (including instances in which the website operates as a "gateway" to  
8 sales), such that the website "is the equivalent of a physical store in California." Since this case involves  
9 illegal conduct emanating from Defendant's operation of its website targeting Californians, California  
10 courts can "properly exercise personal jurisdiction" over the Defendant in accordance with the Court of  
11 Appeal opinion in *Thurston v. Fairfield Collectibles of Georgia*, 53 Cal.App.5th 1231 (2020).

12 3. Venue is proper in this County pursuant to California Code of Civil Procedure section  
13 394(b).

### 14 **III. PARTIES**

15 4. Plaintiff is a resident of California. Plaintiff is also a consumer privacy advocate who  
16 works as a "tester" to ensure that companies abide by the privacy obligations imposed by California  
17 law. As an individual who advances important public interests at the risk of vile personal attacks,  
18 Plaintiff should be "praised rather than vilified." *See Murray v. GMAC Mortgage Corp.*, 434 F.3d 948,  
19 954 (7th Cir. 2006). Indeed, the Ninth Circuit recently made exceptionally clear that it is "necessary  
20 and desirable for committed individuals to bring serial litigation" to enforce and advance consumer  
21 protection statutes, and that Courts must not make any impermissible credibility or standing inferences  
22 against them. *Langer v. Kiser*, 57 F.4th 1085, 1095 (9th Cir. 2023).

23 5. Defendant is a Maryland conglomerate that markets undergarments and related products  
24 via its website throughout the United States and to consumers in this County.

### 25 **IV. FACTUAL ALLEGATIONS**

#### 26 **A. The Right to Privacy Has Always Been a Legally Protected Interest in the United States.**

27 6. Since America's founding, privacy has been a legally protected interest at the local, state,  
28 and federal levels. *See Patel v. Facebook, Inc.*, 932 F.3d 1264, 1271–72 (9th Cir. 2019) (quoting *Spokeo*,

1 *Inc. v. Robins*, 578 U.S. 330, 341 (2016)) (“Privacy rights have long been regarded ‘as providing a basis  
2 for a lawsuit in English or American courts.’”); and *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 983 (9th  
3 Cir. 2017) (“Violations of the right to privacy have long been actionable at common law.”).

4 7. More specifically, privacy protections against the disclosure of personal information are  
5 embedded in California statutes and at common law. *See e.g., U.S. Dep’t of Justice v. Reporters Comm.*  
6 *for Freedom of the Press*, 489 U.S. 749, 763 (1989) (“The Ninth Circuit has repeatedly held that privacy  
7 intrusions may constitute “concrete injury” for purposes of Article III standing); *Van Patten v. Vertical*  
8 *Fitness Grp., LLC*, 847 F.3d 1037, 1041–43 (9th Cir. 2017) (finding “concrete injury” where plaintiffs  
9 claimed that unsolicited telemarketing calls “invade the privacy and disturb the solitude of their  
10 recipients”); *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 599 (9th Cir. 2020) (finding  
11 “concrete injury” where Facebook allegedly tracked users’ “personally identifiable browsing history”  
12 on third party websites); *Patel*, 932 F.3d at 1275 (finding “concrete injury” where plaintiffs claimed  
13 Facebook’s facial-recognition technology violated users’ privacy rights).

14 8. In short, the privacy of personal information is—and has always been—a legally  
15 protected interest in many contexts. Thus, a defendant whose acts or practices violate consumer privacy  
16 inflicts an actionable “injury” upon an individual.

17 **B. Defendant Secretly Attaches Tracking Software to the Devices of All Visitors To Its**  
18 **Website In Violation of California Law.**

19 9. Every device connected to the internet has a unique IP address, typically consisting of a  
20 sequence of numbers. *See United States v. Cairra*, 833 F.3d 803, 805 (7th Cir. 2016). An IP address “is  
21 used to route information between devices.” *United States v. Ulbricht*, 858 F.3d 71, 84 (2d Cir. 2017).

22 10. A “session” represents the time a particular device is connected to a particular website.  
23 Each session reveals information about a user in addition to the unique IP address, such as the user’s  
24 operating system name, operating system version number, browser name, browser version number,  
25 browser language, screen resolution, geolocation data, and device signature.

26 11. Using tracking software, a website owner can gather information from visitor devices  
27 that visit a particular website to create a unique digital profile of each specific website visitor. This  
28 process is known as “digital fingerprinting.”

1           12. If a website owner can link a unique digital profile created by digital fingerprinting to a  
2 particular individual, the website owner can assemble a detailed picture of a person's private life,  
3 including: the online services for which an individual has registered; personal interests based on websites  
4 visited; organizational affiliations; where the individual has been physically; a person's political and  
5 religious affiliations; individuals with whom they have leanings and with whom they associate; and  
6 where they travel, among other things. See [https://www.priv.gc.ca/en/opc-actions-and-](https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2013/ip_201305/)  
7 [decisions/research/explore-privacy-research/2013/ip\\_201305/](https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2013/ip_201305/) (last downloaded January 2024).

8           13. For the preceding reasons, the ability to link a unique digital profile to a specific  
9 individual using digital fingerprinting is of great monetary value. Indeed, it has created an entire industry  
10 known as "identity resolution." Identity resolution is generally defined as "the ability to recognize an  
11 individual person, in real-time, by connecting various identifiers from their digital interactions across  
12 devices and touchpoints." See <https://www.fullcontact.com/identity-resolution/> (last visited January  
13 2024).

14           14. One of the means by which a website owner can gather digital fingerprints as part of its  
15 identity resolution efforts is by deploying "pen register" and/or "trap and trace" spyware (collectively,  
16 "PR/TT spyware") on its website.

17           15. In the past, PR/TT technology required physical machines, but today they take the form  
18 of software. See *In re Order Authorizing Prospective & Continuous Release of Cell Site Location Recs.*,  
19 31 F.Supp.3d 889, 898 n.46 (S.D. Tex. 2014) (citing *Susan Freiwald, Uncertain Privacy: Communication Attributes After the Digital Telephony Act*, 69 S. Cal. L. Rev. 949, 982-89 (1996)  
20 (describing the evolution of PR/TT technology from mechanical device to computer code)).  
21

22           16. In lay terms, PR/TT spyware captures electronic impulses that identify the originating  
23 source of the communication by capturing routing, address, or signaling information. The most common  
24 manner by which this occurs is by obtaining information from targets through location, event, and data  
25 tracking on smart phones along with and data sharing arrangements with third parties.

26           17. Indeed, PR/TT spyware has caught the attention of the United States Director of National  
27 Intelligence, who recently explained that "the advancement of digital technology, including location-  
28 tracking and other features of smartphones and other electronic devices, and the advertising-based

19. The PR/TT beacon on Defendant's website deploys numerous signaling mechanisms to trap and trace users: it monitors user activity (such as page views, searches, or purchases), de-codes the device used by each website visitor, and helps identify the location, race, age, and ethnicity of each user. This data is captured and processed for the purpose of identifying the source of electronic communications on the website for consumer identification purposes.

## Consumer Identity Resolution





21. In the above example, identity resolution has been achieved: using PR/TT spyware materially identical to the technology used by the Defendant, the website owner has gathered and assimilated sufficient digital fingerprints of an anonymous visitor to identify that visitor as Mary Smith, and now knows the following information about her:

- (a) Full name (*Mary Smith*)
- (b) Date of birth (*May 1, 1979*)
- (c) Gender (*female*)
- (d) Home address (*2345 Avenue C, Papillion Nebraska*)
- (e) Marital Status and Family (*Married with two children*)
- (f) E-mail address (*Mary.Smith@gmail.com*)
- (g) Personal Cell Phone: (*(111) 123-4567*)
- (h) Voter Registration Status (*Registered*)
- (i) Interests (*Shopping, Cooking, Traveling, Reading, Science*)
- (j) Employer (*Karen's Fireside, Inc.*)
- (k) Title (*Vice President*)
- (l) Work Hours (*Daily 9-5*)

22. Because of the extraordinary privacy implications and potential for abuse, California law prohibits the deployment of PR/TT spyware without first obtaining a court order. Cal. Penal Code § 638.51 ("CIPA Section 638.51"). CIPA defines a "pen register" broadly to include "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication" *Id.* § 638.50(b). CIPA likewise defines "trap and trace" software broadly to include "a device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, but not the contents of a communication." *Id.* at 638.50(c).

23. CIPA provides for a private right of action and imposes civil liability and statutory penalties for the installation of pen register or trap and trace software without a court order. *Id.*; *see also Greenley v. Kochava*, 2023 WL 4833466, at \*15-\*16 (S.D. Cal. July 27, 2023).



24. As explained above, Defendant knowingly and intentionally deployed PR/TT spyware to (1) decode and record the routing, addressing, and signaling information transmitted by Plaintiff's electronic device communication; and (2) capture the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication. Defendant did so as part of its identity resolution efforts. This conduct constitutes illegal installation of both "pen register" and "trap and trace" software in violation of California law. *See Greenley v. Kochava*, 2023 WL 4833466, at \*15-\*16 (S.D. Cal. July 27, 2023).

25. Defendant did not obtain Plaintiff's knowing and informed consent to the preceding acts, nor did Defendant obtain a court order authorizing it to do so.

26. Plaintiff brings this action as an individual Complaint with the hope that Defendant will voluntarily stop its unlawful conduct, remediate the damage caused, and compensate Plaintiff. If Defendant refuses, Plaintiff will amend this Complaint to name additional plaintiffs and/or add class allegations. Plaintiff does not assert any claims arising under federal law, nor does Plaintiff seek an injunction nor damages in excess of \$75,000, exclusive of interest and costs.

#### V. CAUSE OF ACTION

#### CALIFORNIA INVASION OF PRIVACY ACT

#### PENAL CODE SECTION 638.51

27. Section 638.51 of the Penal Code provides that it is illegal to "install or use a pen register or a trap and trace device without first obtaining a court order pursuant to Section 638.52 or 638.53." (Penal Code § 638.51(a).)

28. Defendant knowingly and criminally deployed pen register and trap and trace software to access Plaintiff's device, install tracking software, and track Plaintiff. *See Greenley v. Kochava*, 2023 WL 4833466, at \*15-\*16 (S.D. Cal. July 27, 2023) (Bashant, J.). Plaintiff did not consent to Defendant's actions.

29. Plaintiff suffered both an economic injury and an intangible injury to Plaintiff's dignity caused by the violation of Plaintiff's right to privacy.

1       30. By knowingly violating a criminal statute and illegally accessing Plaintiff's device to  
2 install tracking software, Defendant acted with oppression and malice. As such, Defendant is liable for  
3 punitive damages pursuant to Civil Code section 3294.

4       31. Plaintiff is also entitled to statutory damages of \$5,000. *See* Penal Code § 637.2(a)(1).

5                               **PRAYER FOR RELIEF**

6       WHEREFORE, Plaintiff seeks judgment against Defendant as follows:

- 7       a. For statutory damages, punitive damages, attorneys' fees, subject to the limiting  
8 paragraph set forth above; and  
9       b. For any and all other relief at law that may be appropriate.

10  
11       Dated: January 18, 2024

PACIFIC TRIAL ATTORNEYS, APC

12                               By: 

13                               Scott. J. Ferrell  
14                               Attorneys for Plaintiff